	Georgia Technology Authority	
Title:	**Bluetooth**	
PSG Number:	SO-06-004.02	**Topical Area:** Service Delivery and Support, Operations Management
Document Type:	Standard	**Pages:** 16
Issue Date:	04/01/06	**Effective Date:** 04/01/06
POC for Changes:	Georgia Wireless Standard Committee	
Synopsis:	Deployment of wireless technology	

STAKEHOLDERS

Name	Stake in Project	Organization	Title
Patrick Moore	Executive Sponsor	Office of the Governor (GOV)	Deputy Chief Operating Officer
Tom Wade	Business Owner	GTA	Chief Executive Officer
Charlie Sasser	Executive Sponsor of Work Group and Wireless Trials	GTA	Director of Support Services
Kimberly Gordon	Subject Matter Expert	GTA	Enterprise Architect
Wireless Oversight Committee	**Executive Committee –** State of Georgia Agencies		Executives from Various Agencies
	Hanna Hecke, GOV Tom Maier, BOR Randall Thursby, BOR Jim Flowers, BOR Mike Hall, DOE John Stewart, DHR Dee Ford, DEcD	Frank Howard, DTAE Mike Nixon, GPB Tony Mazza, P&P Cigdem Delano, GTA Renee Herr, GTA Steve Nichols, GTA Suhas	

			Uppalapati, GTA Robert Woodruff, GTA
ISO Council	Defining and verifying security requirements	State of Georgia Agencies	All Information Security Officers (ISO)
CIO Council	Final approval for operational turnover and Implementation	State of Georgia Agencies	All Chief Information Officers (CIO)
Wireless Standards Work Group	**Team Members –** State of Georgia Agencies		Wireless Experts
	Bruce Bailey, DHR Rory McClure, DHR Walter Tong, DOE Geoff Catron, DTAE Steve Ferguson, DTAE Matt Sanders, GaTech Dan Brown, GEMA Chip Eberhart, GPB Mike Nixon, GPB	Eric Harris, GSP Brent Williams, KSUi Bob Grafals, GTA Chuck Jordan, GTA Denise Techmeier, GTA, Program Technical Writer Jim Mollohan, GTA, Program Business Owner Wray Hall, GTA	

[i] Kennesaw State University

[ii] The 802.15 WPAN™ effort focuses on the development of consensus standards for Personal Area Networks or short distance wireless networks. These WPANs address wireless networking of portable and mobile computing devices such as PCs, Personal Digital Assistants (PDAs), peripherals, cell phones, pagers, and consumer electronics; allowing these devices to communicate and interoperate with one another. The goal is to publish standards, recommended practices, or guides that have broad market applicability and deal effectively with the issues of coexistence and interoperability with other wired and wireless networking solutions.

[iii] IEEE, pronounced I-triple-E, was founded in 1884 as the AIEE. The IEEE was formed in 1963 when AIEE merged with IRE. IEEE is an organization composed of engineers, scientists and students. The IEEE is best known for developing standards for the computer and electronics industry. In particular, the IEEE 802 standards for local-area networks are widely followed.

PURPOSE

To define 802.15ii standards for agencies to use in deployment of wireless technology.

INDUSTRY STANDARD

This standard applies to the use of wireless technologies deployed on an agencies' wireless personal area network. The dominant standards to date have been the 802 standards series developed by the Institute of Electrical and Electronic Engineersiii (IEEE). Any use of wireless strategy should comply with the most current version of the IEEE 802.15 standard. The current version of 802.15 can be found at http://grouper.ieee.org/groups/802/15/. To further standardize the use and deployment of 802.15 in the State of Georgia's environment, the following areas are clarified in this policy adoption: establishing a net, link encryption, degradation and coexistence.

Although many government entities have already started using wireless technology, the intent of this document is to outline areas that need to be reviewed and explain areas that need to be considered on initial deployment.

The following standards are in commercial, office and industrial use: IEEE's 802.15.1, 802.15.2, 802.15.3 and 802.15.4. These standards will serve as the de facto Wireless Personal Area Network standards for the State. Whenever deploying a WPAN solution, agencies must insure vendors meet these standards. A summary of the standards and a comparative table are below. This document will be updated as applicable standards are ratified by IEEE.

IEEE 802 Standard	Name	Description
802.15.1 & 802.15.1a	WPAN or Bluetooth	Bluetooth wireless technology operates in the 2.4-gigahertz (GHz) Industrial, Scientific and Medical (ISM) band (from 2.4 to 2.4835 GHz), dividing this frequency range into 79 1-megahertz (MHz) subchannels and hopping from channel to channel 1,600 times per second. Transmitting and receiving devices must synchronize on the same hop sequence to communicate. The technology has a maximum theoretical data rate of 1 Mbps. Actual maximum throughput is approximately 400–700 Kbps, depending on the channel configuration. Bluetooth links are short range, designed to link personal electronics devices that are fairly close together— typically no more than 10 meters (or approximately 30 feet). Unlike Infrared Data Association (IrDA) devices, a Bluetooth link does not require that the devices be lined up precisely within line-of-sight of each other. Bluetooth wireless technology may offer more flexibility than the IrDA ports on portable computers, mobile phones, and PDAs. Bluetooth is designed for cable replacement in a short-range, personal area network. Bluetooth eliminates cabling between electronic products and accessories and is more oriented toward user mobility and eliminating short distance cabling. Bluetooth users with handhelds or laptops can exchange files, business cards and calendar appointments. 802.15.1a incorporates changes to 802.15.1 based on Bluetooth version 1.2
802.15.2	Coexistence	Determine methods of allowing coexistence between Bluetooth WPANs and WLANs based on 802.11g and 802.11b

802.15.3 & 802.15.3a	WPAN High Rate & WPAN Alt High Rate PHY	The 802.15.3 standard allows data to be transmitted in the 2.4GHz frequency band at 55 Mbps with a range of 300 feet/100 meters. Networks using 802.15.3 also will be able to switch channels automatically if interference from cordless phones or other networks is detected. The 802.15.3 network was designed to coexist with other wireless technologies such as Bluetooth, 802.11, and WiFi. Develops a high rate physical layer operating at 11,22,33,44 and 55 Mps. 802.15.3 provides a high-speed physical layer for 802.15.3 to support applications that involve imaging and multimedia.
IEEE 802 Standard		**Description**
802.15.4	WPAN Low Rate	The 802.15.4 standards define the ZigBee network, which supports security and reliability, low data rates, and low power consumption. ZigBee will be able to implement star and mesh network topologies, a variety of data security features, and interoperable application profiles. ZigBee addresses most remote monitoring and control and sensory network applications. ZigBee protocols define a type of sensor network for residential and commercial applications such as heating, air conditioning and lighting control. It combines IEEE 802.15.4, which defines the physical and MAC protocol layers, with network, security and application software layers as specified by the ZigBee Alliance, a consortium of technology companies. ZigBee aims more for grand-scale automation and remote control. Investigates a low-data-rate solution with multimonth to multiyear battery life and very low complexity. It is intended to operate in an unlicensed international frequency band. Potential applications are sensors, interactive toys, smart badges, remote controls and home automation.

Capability Comparison

	Bluetooth	Zigbee
Modulation	Frequency Hopping Spread Spectrum (FHSS)	Direct Sequence Spread Spectrum (DSSS)
Protocol stack size	250K bytes	28K bytes
Battery	Intended for frequent recharging	Not rechargeable
Maximum network speed	1M bit/sec	250K bit/sec
Network range	1 or 100 meters, depending on radio class	Up to 70 meters
Typical network join time	3 seconds	30 milliseconds

STANDARD FOR THE STATE OF GEORGIA

In order to address the risks associated with wireless computer networks, the State of Georgia has established a wireless network access policy (Policy 9.4.2). The policy requires agencies to take "appropriate steps, including the implementation of strongest-available encryption, user authentication, and virus protection measures, to mitigate risks to the security of State of Georgia data and information systems . . . ." the State of Georgia's standards require agencies to develop a wireless LAN Implementation Procedure Plan, assess the risks posed by a wireless network, mitigate those risks, and conduct periodic reviews to ensure that the network is secure. The standards prohibit open unsecured wireless network access technology.

The ISO Council has adopted the National Institute of Standards and Technology (NIST) 800 series as the security guidelines. Wireless security is specifically addressed in the following NIST standards:

- NIST 800-18 Guide for Developing Security Plans for IT Systems;
- NIST 800-46 Security for Telecommuting and Broadband Communications; and
- NIST 800-48 Wireless Network Security: 802.11, Bluetooth and Handheld Devices.

Use 802.3f, specification of Power over Ethernet (PoE), to enhance AP operation via a stable power source and simplify installation process throughout the enterprise.

Wireless Local Area Networks (WLANs) should at the minimum implement WPA (Wireless Protected Access) for security, but full 802.11i compliance is a standard

with components and equipment that can adhere to 802.11i.

For areas not mentioned in this section, seek guidance in the external sources mentioned in the “Standards” section.

Bluetooth will continue to be a cable replacement and short-range network technology. Bluetooth comes up short on range and speed for general LAN use, consequently, it should be used as peripheral support and synchronization of handheld devices (PDAs, cell phones, etc.).

Use Bluetooth 2.0 to:

- transport authentication credentials or “smart card” functions, allowing a wide range of commercial transactions to take place;
- eliminate the spaghetti bundle of wires that connects peripheral devices to desktops and laptops;
- replace inter-device cables
- handle two-way nature of the communication;
- allow wireless connections between headsets and cellular phones; and
- enable communications functions of various devices outside of “cable range” optimize for voice and other low-data-rate application and QoS

When deploying Bluetooth and 802.11g in the same device, make sure the implementation of both wireless technologies includes a coexistence solution.

1.1 SECURITY

Use either of the modes listed based on the data, network or device that needs to be secure:

- Service-level enforced security: A device does not initiate security procedures before establishing a connection. This mode allows flexible access policies for applications, especially when running applications with different security requirements in parallel.
- Link-level enforced security: A device initiates security procedures before a link is established.
- Use an alternative protocol for the exchange of PIN codes
- Use application-level (on top of the Bluetooth 2.0 stack) encryption and authentication for highly sensitive data communication.
- Install antivirus software on intelligent, Bluetooth-enabled hosts.
- Fully test and deploy software Bluetooth patches and upgrades regularly.
- Deploy user authentication such as biometrics, smart cards, two-factor authentication or PKI.
- Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.

1.2 RISK MITIGATION

In mitigating the risks associated with wireless computer networks, all state agencies should:

- Monitor the random generator. The Random Number Generator (RNG)

may produce static number or periodic numbers that may reduce the effectiveness of the authentication scheme.
- Enforce the length of user's PINs. Weak PINs, which are used for the generation of link and encryption keys, can be easily guessed. Increasing the PIN length in general increases the security.
- Encrypt key length. Develop a more robust encryption procedure.
- Develop user authentication on application level.
- Frequently change the Bluetooth device address (BD_ADDR). Once the BD_ADDR is associated with a particular user, that user's activities could be logged, resulting in a loss of privacy.
- Use of mutual authentication is required to provide verification that users and the network are legitimate.
- Develop procedures for End-to-end security.
- Agencies using Bluetooth technology need to establish and document security policies that address the use of Bluetooth-enabled devices and the user's responsibilities. The policy document should include a list of approved uses for Bluetooth networks, the type of information that may be transferred in the network, and any disciplinary actions that may result from misuse. The security policy should also specify a proper password usage scheme.
- Establishment of spatial distance and securing the gateway of Bluetooth devices that remotely connect to the network should be analyzed at the agency level.
- Agencies with requirements for high levels of security should also restrict unauthorized personnel from using PDAs, laptops other electronic devices within the secure perimeter.
- Because the PINs are necessary for authentication and for link security, administrators should ensure that Bluetooth devices are not using default PINS, or lowest setting (e.g., 0000).
- Since Bluetooth devices can store and automatically access link-level PINs from memory, a Bluetooth device should employ device authentication as an extra layer of security. Incorporating application-level software that requires password authentication to secure the device will add an extra layer of security. Agencies with both high-end users and low-end users should incorporate application-level software that requires password authentication in Bluetooth devices.

1.3 AUDITING

The some of the areas that will be reviewed during an audit are listed below.

- Was Bluetooth 2.0 used when wired networks were not available? Make sure that the technology was not used in linking computers, in operation in large-scale WLAN deployments or in out-of-the-box security needs.
- Has ample work been done to delete or eliminate degradation? In a dense Bluetooth environment, where many devices are within a few feet of each other, 802.11b/g may experience degraded operations. The degradation depends on the number of Bluetooth devices in

proximity to the 802.11b/g transceiver and the amount of interference from other signal sources in the 2.4GHz ISM band. Bluetooth and 802.11b/g networks can coexist well. Only when Bluetooth and 802.11b/g radios are within a few inches of each other will significant interference be noticed, although the distance at which interference begins will be based on the presence of other signals in the 2.4 GHz band. Since Bluetooth uses frequency-hopping spread spectrum (FHSS) modulation, most often significant interference will be experienced by other FHSS technologies, such as cordless telephones and baby monitors.

- Did the deployment enforce user-based authentication and access control within the Bluetooth 2.0 security framework? The Bluetooth 2.0 architecture allows for defining security policies that can set trust relationships in such way that even trusted devices can get access only to specific services.

EXCEPTIONS

All exceptions to this standard need to be approved by GTA.

GUIDELINES

Best Practice #1: Enabling Bluetooth 2.0

As with other wireless technologies, Bluetooth should not be active when authentication is disabled. If Bluetooth is not to be used on a particular device, make sure Bluetooth is disabled.

Best Practice #2: Training

Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology.

Best Practice #3: Assessments

Perform a risk assessment to understand the value of the assets in the agency that need protection. Perform comprehensive security assessments at regular intervals to fully understand the wireless network security posture.

Best Practice #4: Devices

Ensure that handheld or small Bluetooth devices are protected from theft. Ensure that Bluetooth devices are turned off during all hours when they are not used. Study and understand all planned Bluetooth-enabled devices to understand any security idiosyncrasies or inadequacies. Change the default settings of the Bluetooth device to reflect the agency's security policy. Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the agency. Ensure that portable devices with Bluetooth interfaces are configured with a password to prevent unauthorized access if lost or stolen.

Best Practice #5: PIN codes

Choose PIN codes that are sufficiently random and avoid all weak PINs. Choose PIN codes that are sufficiently long (maximal length if possible). Ensure that no Bluetooth device is defaulting to the zero PIN. Configure Bluetooth devices to delete PINs after initialization to ensure that PIN entry is required every time and that the PINs are not stored in memory after power removal.

Best Practice #6: Encryption

Invoke link encryption for all Bluetooth connections regardless of how needless encryption may seem. Ensure that encryption is enabled on every link in the communication chain. Enable encryption for all broadcast transmissions. Configure encryption key sizes to the maximum allowable. Establish a "minimum key size" for any key negotiation process.

TERMS and DEFINITIONS

Bluetooth

Bluetooth 2.0 is a specification that provides a low-cost, low-power radio frequency solution for wireless transmission between a wide variety of devices, including PCs, keyboards, cordless telephones, cell phones, headsets, printers, monitors, LCD projectors, and PDAs. Unlike WiFi, which specializes in enabling high data-rate WLANs over distances of up to 100 km, Bluetooth was developed to take advantage of point-to-point personal area network (PAN) connections over short distances, typically ranging from 10 to 100 meters. Compared with the lowest grade of WiFi, 802.11b, which provides data transmission rates of approximately 5.5 M bps, Bluetooth's gross data rate has been only 1M bps under ideal circumstances. While Bluetooth may lag in connection distance and throughput rates, the specification excels as a low-power means of connecting and transferring data between small, battery-powered portable devices, such as personal digital assistants and cellular phones. Bluetooth 2.0 offered speeds three to ten times more than the original specification.

The baseband controller and radio are the heart of the Bluetooth hardware solution. Because of the controller's small size, low cost, and low power requirements, it can be incorporated into many electronic devices or appliances. It is ideal for PDAs with their small form factor and low power requirements. It can also be implemented on a USB device (or "dongle"), PC Card, or PC system board.

Bluetooth networks can support either one asynchronous data channel with up to three simultaneous synchronous speech channels or one channel that transfers asynchronous data and synchronous speech simultaneously. Bluetooth uses a combination of packet-switching technology and circuit-switching technology. The advantage of using packet switching in Bluetooth is that it allows devices to route multiple packets of information by the same data path. Since this method does not consume all the resources on a data path, it becomes easier for remote devices to maintain data flow throughout a scatter-net. The three ranges for Bluetooth are:

Class 1 Devices High 100 mW (20 dBm) Up to 100 meters (300 feet)
Class 2 Devices Medium 2.5 mW (4 dBm) Up to 10 meters (30 feet)
Class 3 Devices Low 1 mW (0 dBm) 0.1–10 meters (less than 30 feet)

The shortest range may be good for applications such as cable replacement (e.g., mouse or keyboard), file synchronization, or business card exchange. The high-powered range can reach distances of 100 m, or about 300 ft. Additionally, as with the data rates, it is anticipated that even greater distances will be achieved

in the future.

iDEN

iDEN (Integrated Digital Enhanced Network) is a mobile communications technology that provides its users with the benefits of a trunked radio and a cellular telephone. iDEN places more users in a given spectral space, as compared to analog cellular systems, by using Time Division Multiple Access (TDMA). Six communication channels share a 25 kHz space. Some competing technologies place only one channel in 12.5 kHz. Data (such as paging, text messaging and voice communications) are supported by iDEN. iDEN is a technology with no clear path for high speed wireless data.

Interface

A protocol of behavior that can be implemented by any class, anywhere in the class hierarchy. An interface defines a set of methods, but does not implement them. A class that implements the interface agrees to implement all the methods defined in the interface, thereby agreeing to certain behavior.

MAC

The Media Access Control address is a unique numeric identifier that is programmed into a wireless network interface card by the manufacturer. Some manufacturers allow this identifier to be reprogrammed by the user, therefore it must be assumed that the MAC address can be copied electronically (spoofed).

Mobile

Specification of physical and medium access control layers of an air interface for interoperable mobile broadband wireless access systems. These systems operate in licensed bands below 3.5 GHz, optimized for IP-data transport, with peak data rates per user in excess of 1 Mbps. This specification supports various vehicular mobility classes up to 250 Km/h in a MAN environment and targets spectral efficiencies, sustained user data rates and numbers of active users that are all significantly higher than those achieved by existing mobile systems.

Piconet

A piconet is formed when a user begins the “pairing” process between two Bluetooth devices. The user is prompted to enter the personal identification number (PIN) of each device during pairing in order to establish initial authentication and encryption keys. After pairing is complete, the two devices recognize each other and are entered in the respective “trusted partners” database on each device.

In forming a piconet, a master unit gives the slave units its clock and 48-bit device ID. The device ID comes from the global address space used to create MAC addresses for Ethernet and other networking technologies. The device ID determines the hopping pattern, while the clock determines the phase within the hopping pattern. Slave units may communicate with multiple master units,

as occurs in a scatternet environment.

To keep track of active and parked devices within the piconet, the protocol uses 11 bits. The active member address (AMA) is three bits long, while the parked member address (PMA) is eight bits long. This corresponds to the limit of 7 active and 200 parked devices.

WEP

Wired Equivalent Privacy, (WEP) a security protocol based on RC4 encryption algorithm, is built into the IEEE 802.11standards for wireless LANs. This standard does not use a FIPS-validated crypto module, and has been found by the cryptographic community to have fundamental flaws. Protected Access (WPA) version 1, WPA2 (WPA version 2) is a newer security protocol built into the 802.11i standard. It offers better protection using temporal key integrity protocol (TKIP). This protocol was added, so that keys are rotated and encryption is strengthened, but it is still based on the RC4 encryption algorithm. WPA2 version 2 of WPA will use strong AES encryption based on Rijndael algorithm (128, 192 or 256 bit key sizes). WPA2 also adds two strong authentication features: wireless robust authentication protocol or (WRAP), counter with cipher block chaining message authentication code protocol or (CCMP).

WiDen

A software upgrade developed for iDEN enhanced specialized mobile radio (or ESMR) wireless telephony protocol. WiDEN allows compatible subscriber units to communicate across four 25 kHz channels combined for up to 100 kbit/s of bandwidth. The protocol is generally considered a 2.5G wireless cellular technology.

WiFi

Wireless Fidelity is another name for wireless devices running under the 802.11b standard, which operates in the 2.4 GHz range. The name is governed (or marketed) by the Wireless Ethernet Compatibility Alliance (WECA).

5, or 5, is a newer version for devices running under the faster 802.11a standard. It operates in the 5 MHz range. Specifically, 5.15 MHz to 5.35Mhz for indoor use, and 5.725 MHz to 5.825 MHz for outdoor use.

-x is a generic name for devices that support 802.11b and 802.11a.

WMAN

Metropolitan Area Networks (MANs) are large computer networks usually spanning a campus or a city. They typically use optical fiber connections to link their sites. For instance, a university or college may have a MAN that joins together many of their local area networks (LANs) situated around a site that is a fraction of a square kilometer. Then from their MAN, they could have several Wide Area Network (WAN) links to other universities or the Internet. Some technologies used for this purpose are ATM, FDDI and SMDS. These older technologies are in the process of being displaced by Gigabit

Ethernet-based MANs in most areas. MAN links between LANs have been built without cables using either microwave, radio, or infra-red free-space optical communication links.

WiMAX

WiMAX is another name for a set of broadband wireless communication standards, developed under IEEE 802.16, for metropolitan area networks. Originally called WirelessMANT, the name is governed (or marketed) by the WiMAX Forum. This forum was founded by a coalition of wireless companies including Intel, Proxim, and Nokia. (Nokia has now left.) WiMAX was ratified as a standard under the 802.16-2004 specification.

WiMAX is expected to compliment standards. It provides a wireless alternative to last mile local loops, such as T-1 links. WiMAX should also provide competition for broadband DSL and cable services.

Wireless

Term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part, or all, of the communication path. Some monitoring devices, such as intrusion alarms, employ acoustic waves at frequencies above the range of human hearing; these are also sometimes classified as wireless.

WLAN

A Wireless Local Area Network (Wireless LAN) is a computer network that allows a user to connect without a network cable. A laptop or PDA equipped with a wireless LAN card allows a user move around a building with their computer and stay connected to their network without needing to “plug in” with a cable. The most popular wireless LAN today is called an 802.11b network. Wireless LANs require an access point where all the wireless devices connect. This connection point connects the users to the wired network. The coverage of a wireless access point can span up to 100 m (330 feet) indoors.

Other names for wireless LANs are 802.11, or WiFi. There are also different versions of wireless LANs: 802.11b transfers data at speeds of up to 11 Mbps in the 2.4 GHz radio band. The next version, 802.11a, is supposed to transfer data at speeds up to 54 Mbps in the 5 GHz band. Wireless LANs are a successful and popular widespread technology that is being incorporated into many new laptops as standard equipment.

WPA

WPA (WiFi Protected Access) is an interim standard by the Alliance. Protected Access is a specification of security enhancements that increases the level of data protection and access control for existing networks.

WPA will most likely be rolled into the eventual IEEE 802.11i standard.

WPA2

IEEE 802.11i (also known as WPA2) is an amendment to the 802.11 standard specifying security mechanisms for wireless networks (see WiFi). The draft standard was ratified on 24 June, 2004, and supersedes the previous security specification, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses. WiFi Protected Access (WPA) had previously been introduced by the WiFi Alliance as an intermediate solution to WEP insecurities. It implemented a subset of 802.11i

WPAN

Wireless Personal Area Network (WPAN) is a personal area network that is used for interconnecting devices centered on an individual person's workspace where the connections are wireless. Typically, a wireless personal area network uses some technology that permits communication within about a very short range, such as 10 meters. One such technology is Bluetooth, which was used as the basis for a new standard, IEEE 802.15.

A WPAN can interconnect all the ordinary computing and communicating devices that many people have on their desk or carry with them today. It can also serve a more specialized purpose such as allowing a surgeon and other team members to communicate during an operation.

A key concept in WPAN technology is plugging in. In the ideal scenario, when any two WPAN-equipped devices come into close proximity (within several meters of each other), or within a few kilometers of a central server, they can communicate as if they are connected by a cable. Another important feature is the ability of each device to lock out other devices selectively, preventing needless interference or unauthorized access to information.

The technology for WPANs is in its infancy and is undergoing rapid development. Proposed operating frequencies are around 2.4 GHz in digital modes. The objective is to facilitate seamless operation among home or business devices and systems. Every device in a WPAN will be able to plug in to any other device in the same WPAN, provided they are within physical range of one another. In addition, WPANs worldwide will be interconnected.

WWAN

A Wireless Wide Area Network (Wireless WAN), covers a much more extensive area than wireless LANs. Coverage is generally offered on a nationwide level with wireless network infrastructure provided by a wireless service carrier (for a monthly usage fee, similar to a cellular phone subscription). While wireless LANs are used to allow network users to be mobile within a small fixed area, wireless WANs are used to give Internet connectivity over a much broader coverage area. For instance to meet the requirements of users such as business travelers or field service technicians. Wireless WANs allow users to have access to the Internet, e-mail, and corporate applications and information while away from their office. Wireless WANs use cellular networks for data transmission. A portable computer with a wireless WAN modem connects to a base station on the wireless networks via radio waves. The radio tower then carries the signal to a mobile switching center, where the data is passed on to the appropriate network. Using the wireless service provider's connection to the Internet, data communications are established to an organization's existing network. Wireless WANs use existing cellular telephone networks, so there is also the option of making voice calls over a wireless WAN. Both cellular telephones and wireless WAN PC Cards have the ability to make voice calls as well as pass data traffic on wireless WAN networks.

Zigbee

Bluetooth and ZigBee have much in common. Both are types of IEEE 802.15 "wireless personal-area networks," or WPANs. Both run in the 2.4-GHz unlicensed frequency band, and both use small form factors and low power.

Note: PSG number administratively changed from S-06-004.02 on September 1, 2008.